УДК 343.98

ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРПРЕСТУПНОСТИ В ЭКОНОМИЧЕСКОЙ СФЕРЕ НА СОВРЕМЕННОМ ЭТАПЕ

Д. А. Свиридов
начальник кафедры уголовного процесса и криминалистики,
Могилевский институт МВД Республики Беларусь
e-mail: dima.sviridov@inbox.ru

Аннотация. *В статье рассматриваются общие тенденции трансформации киберпреступности в сфере экономических отношений на современном этапе. Определяются наиболее значимые характеристики киберпреступности, определяющие дальнейшее ее развитие. Делается вывод о том, что на современном этапе киберпреступность вышла на качественно новый — «профессиональный» — уровень, что повышает сложность раскрытия и расследования киберпреступлений, требует транснационального взаимодействия и разработки методов борьбы «на опережение».*

Ключевые слова: *киберпреступность, хакер, транснациональность, кибератака, экономические отношения, борьба с преступностью.*

Annotation. *The article discusses the general trends in the transformation of cybercrime in the field of economic relations at the present stage. The most significant characteristics of cybercrime are determined, which determine its further development. It is concluded that at the present stage, cybercrime has reached a qualitatively new — «professional» — level, which increases the complexity of the disclosure and investigation of cybercrime, requires transnational interaction and the development of «proactive» methods of fighting.*

Keywords: *cybercrime, hacker, transnationality, cyberattack, economic relations, the fight against crime.*

В настоящее время под влиянием процессов глобализации происходит активизация экономической преступности, которая выводит ее на абсолютно новый уровень, расширяя и значительно усложняя само понимание данной категории. Экономическая преступность трансформировалась в серьезную мировую проблему, которая способна влиять не только на экономику отдельных стран, но и негативно сказываться на развитии мировой экономики. Одной из граней данной категории является в том числе киберпреступность, ставшая возможной в результате стремительного развития информационных технологий. Эти самые информационные технологии, которые в настоящее время выступают неотъемлемыми элементами практически каждого человека, общества и государства, положили начало формированию качественно новому виду преступности в сфере экономики. При этом следует отметить справедливую точку зрения В. А. Номоконова и Т. Л. Тропининой, которые указывают, что в современных реалиях Интернет в преступных целях уже дав-

но используется в качестве места и главного средства совершения уже традиционных преступлений (кража, мошенничество, вымогательство и ряд иных), а не только как вспомогательное средство [1, с. 53].

Видится необходимым провести анализ современного состояния и тенденций развития киберпреступности в сфере экономических отношений на фоне стремительного развития коммуникационных и информационных технологий, понимание закономерностей которых позволит понять сущность данного явления и выработать действенные механизмы раннего выявления, раскрытия, расследования и предупреждения такого рода преступлений.

Нельзя отрицать тот факт, что киберпреступность является следствием появления международных компьютерных сетей и развития информационных и коммуникационных технологий [2, с. 119]. Экономическая киберпреступность на современном этапе — быстрорастущий сегмент (прогрессивное увеличение пользователей сети Интернет, совершенствование профессионализма киберпреступников, совершенствование и развитие информационных технологий и обеспечения). Следует отметить, что, насколько полезны ни были любые технические и информационные новшевства, они все равно в той или иной мере расширяют и сферу киберпреступности, создавая дополнительные возможности хакерских атак. По данным Международного союза электросвязи, по состоянию на конец 2019 года пользователями глобальной сети Интернет стали 4,1 млрд человек или 53,6 % населения мира [3].

Помимо трансформации непосредственных форм киберпреступности, происходит смещение акцента на характеристиках личности «хакера». В частности, на современном этапе в качестве основы работы таких лиц лежит преступный бизнес, в том время как еще 15–20 лет назад в основе лежало желание «продемонстрировать» свои умения и навыки при совершении кибератак. Происходит определенное выделение из среды «хакеров» — профессионалов высшей категории, которые самостоятельно обеспечивают себя необходимыми программными средствами и владеют полной информацией о всех процессах при выполнении тех или иных противозаконных операций, и на лиц, которые просто используют приобретенные программные средства в целях обогащения, мести, хулиганства и в иных целях.

Киберпреступность в силу определенных причин, которые позволяют ей оставаться в зоне относительной ненаказуемости, но в то же время достаточной прибыльности, является весьма интересным видом деятельности. Стремительное распространение глобальной сети Интернет повлекло трансформацию киберпреступности с уровня национального на уровень глобальный — лицо, совершающее киберпреступления, может их совершать на территории одного государства, проживать во второй стране, иметь гражданство третьей, а рабо-

тать через сервер, расположенный в четвертой, что позволяет зачастую безопасно для преступника обналичивать денежные средства на безопасных расстояниях от места совершения преступления. Данное положение в том числе свидетельствует о сложности расследования такого рода преступлений и невозможности производства по ним исключительно правоохранительными силами одного государства. Совершение преступных действий зачастую неочевидно, в результате чего жертва может обнаружить факт совершения преступления через довольно длительный промежуток времени, что также не способствует раскрытию такого рода преступлений. Продолжительность кибератак может варьироваться от мгновений до нескольких месяцев, используя в этих целях большое число компьютеров. Так, видится верным привести несколько примеров. Взлом агенства Equifax, которое является одной из трех организаций, ведущих кредитные истории. Как результат взлома в 2017 году произошло хищение данных (личные данные, номера полисов социального страхования, банковских счетов, водительских прав) у 148 млн пользователей — граждан Великобритании, Канады, США. При этом следует иметь в виду, что подсчитать вред достаточно проблематично, так как последствия такого рода взлома могут проявляться достаточно длительное время. В частности, агенство Equifax заявило об ущербе на сумму 600 млн долларов США. Еще одним примером можно привести атаку сетевого червя WannaCry в 2017 году — в зоне заражения оказалось примерно полмиллиона компьютеров не только простых пользователей и частных компаний, но и государственных учреждений. Червь шифровал файлы, после чего пользователю предлагалось заплатить определенную сумму в биткоинах, чтобы получить ключ доступа к шифру [4].

Формы киберпреступности с развитием науки и техники также не стоят на месте и воздействуют на все современные достижения. В настоящее время повышенное внимание нацелено на мобильные устройства и социальные сети. Кибератаки становятся все более сложными, зачастую направлены и на объекты повышенной опасности, такие как атомные электростанции. При этом следует отметить финансовую направленность киберпреступности, т. е. не создание бот-сетей, атакующих неопределенный круг пользователей ради самого причинения вреда, а целевые атаки на конкретных лиц и организации. Для этого необходим сложный комплекс мер, направленных на изучение объекта нападения, его систем защиты, уязвимых мест, неожиданная атака с прикрытием от обнаружения. Как результат — сложности фиксации, сложности при доказывании самого преступления, сложности персонификации преступника и его местонахождения.

По-прежнему в числе лидеров в перечне киберпреступлений остается интернет-банкинг, что связано с возможностью быстрого обогащения. При этом

правонарушителей не смущает тот факт, что банковские учреждения зачастую оборудованы различного рода системами защиты. Снижение стоимости оказываемых услуг за счет внедрения электронных технологий одновременно расширяет возможности для преступников при совершении противоправных финансовых операций. При этом киберпреступники обогащаются посредством различных форм: вымогательство (посредством шантажа похищенной информацией), снятие денежных средств со счетов банков. В связи с этим банковские учреждения и иные кредитно-финансовые организации вынуждены постоянно совершенствовать комплексную защиту дистанционного управления от вредоносного программного обеспечения с целью предотвращения утечки персональной информации.

Сегодня уже очевиден факт невозможности противостоять экономическим киберпреступлениям только лишь на государственном уровне, без взаимодействия с международными организациями, правоохранительными органами других государств, постоянного совершенствования законодательства. Следует понимать, что в целях эффективного противостояния такого рода преступлениям требуется многоуровневая система кибербезопасности, которая включала бы разнообразные компоненты, в т. ч. повышение базового уровня цифровой грамотности населения, механизмы противодействия и профилактики киберугроз, продвижение способов защиты личной информации [5, с. 48].

Таким образом, на основании вышеизложенного сделаем следующие выводы: киберпреступность в настоящее время вышла на новый уровень существования, миновав стадию становления; изменился тип киберпреступника — становление преступника-профессионала, наносящего значительный вред при минимальном риске. Киберпреступность развивается интенсивнее развития существующих систем безопасности. Решение данной проблемы видится возможным на современном этапе не в попытках блокировать выявленные формы киберпреступности, а в активной разработке стратегии информационной безопасности на опережение на основе транснационального сотрудничества.

1. Номоконов В. А., Тропинина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1 (24). С. 45–55. Вернуться к статье

2. Тарасов А. Электронный банкинг и его безопасность // Экономическая политика. 2010. № 5. С. 118–128. Вернуться к статье

3. Committed to connecting the world [Электронный ресурс] / ICT STATISTICS. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (дата обращения: 20.02.2020). Вернуться к статье

4. 5 самых громких кибератак последнего десятилетия [Электронный ресурс] / TECH. URL: https://techrocks.ru/2018/09/26/5-most-celebrated-cyber-attacks (дата обращения: 22.02.2020). Вернуться к статье

5. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46–50. Вернуться к статье